4IPv6、多播、VPN

2019年6月16日 21:29

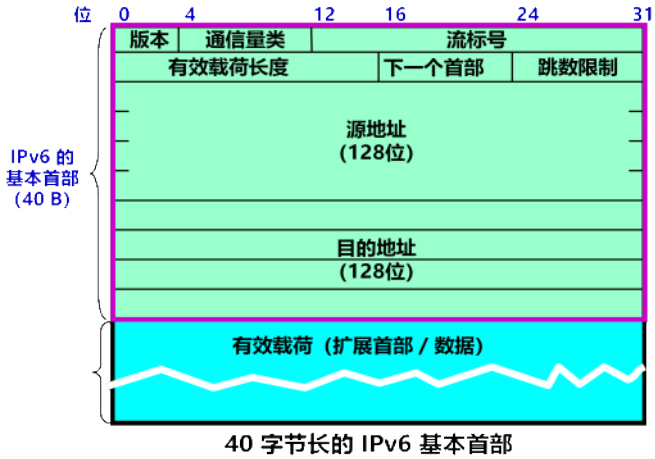
-
- IPv6

1. 到 2011 年 2 月，IPv4 的 32 位地址已经耗尽。
2. ISP 已经不能再申请到新的 IP 地址块了。
3. 我国在 2014 – 2015 年也逐步停止了向新用户和应用分配 IPv4 地址。
4. 解决 IP 地址耗尽的根本措施就是采用具有更大地址空间的新版本的 IP，即 IPv6。

1- IPv6首部

1. IPv6 仍支持无连接的传送，但将协议数据单元 PDU 称为分组。为方便起见，本书仍采用数据报这一名词。所引进的主要变化如下：
   (1) 更大的地址空间：IPv6 将地址从 IPv4 的 32 位 增大到了 128 位。
   (2) 扩展的地址层次结构。
   (3) 灵活的首部格式： IPv6 定义了许多可选的扩展首部。
   (4) 改进的选项： IPv6 允许数据报包含有选项的控制信息，其选项放在有效载荷中。
   (5) 允许协议继续扩充。
   (6) 支持即插即用（即自动配置）：因此 IPv6 不需要使用 DHCP。
   (7) 支持资源的预分配： IPv6 支持实时视像等要求，保证一定的带宽和时延的应用。
   (8) IPv6 首部改为 8 字节对齐：首部长度必须是 8 字节的整数倍（默认40，可在有效载荷中扩展）。原来的 IPv4 首部是 4 字节对齐。
2. 数据报途中经过的路由器都不处理这些扩展首部（只有一个首部例外，即逐跳选项扩展首部），这样就大大提高了路由器的处理效率。

(1)



40 字节长的 IPv6 基本首部

3. 扩展首部：逐跳选项、路由选择、分片、鉴别、封装安全有效载荷、目的站选项

2- IPv6的地址：单播、多播、任播

1. 结点和接口
   (1) IPv6 将实现 IPv6 的主机和路由器均称为结点
   (2) 一个结点就可能有多个与链路相连的接口

(3) IPv6 地址是分配给结点上面的接口的

1) 一个接口可以有多个单播地址

2) 其中的任何一个地址都可以当作到达该结点的目的地址。即一个结点接口的单播地址可用来唯一地标志该结点

2. colon hexadecimal notation冒号十六进制记法

(1) 形如68E6:8C64:FFFF:FFFF:0:1180:960A:FFFF

(2) 允许将一连串连续0用双冒号取代

(3)

地址类型	二进制前缀
未指明地址	**00…0（128位），可记为 ::/128。**
环回地址	**00…1（128位），可记为 ::1/128。**
多播地址	**11111111（8位），可记为 FF00::/8。**
本地链路单播地址	**1111111010（10位），可记为 FE80::/10。**
全球单播地址	**（除上述四种外，所有其他的二进制前缀）**

3. IPv4向v6的过渡

(1) dual stack双协议栈：在完全过渡到 IPv6 之前，使一部分主机（或路由器）装有两个协议栈，一个 IPv4 和一个 IPv6

1) 双协议栈的主机（或路由器）记为 IPv6/IPv4，表明它同时具有两种 IP 地址：一个 IPv6 地址和一个 IPv4 地址

2) 双协议栈主机在和 IPv6 主机通信时是采用 IPv6 地址，而和 IPv4 主机通信时就采用 IPv4 地址

3) 根据 DNS 返回的地址类型可以确定使用 IPv4 地址还是 IPv6 地址

(2) 隧道技术：在 IPv6 数据报要进入 IPv4 网络时，把 IPv6 数据报封装成为 IPv4 数据报，整个的 IPv6 数据报变成了 IPv4 数据报的数据部分；当 IPv4 数据报离开 IPv4 网络中的隧道时，再把数据部分（即原来的 IPv6 数据报）交给主机的 IPv6 协议栈

4. ICMPv6：IPv6 也不保证数据报的可靠交付，因为互联网中的路由器可能会丢弃数据报。因此 IPv6 也需要使用 ICMP 来反馈一些差错信息。新的版本称为 ICMPv6

(1) 地址解析协议 ARP 和网际组管理协议 IGMP 协议的功能都已被合并到 ICMPv6 中

(2) ICMPv6 是面向报文的协议，它利用报文来报告差错，获取信息，探测邻站或管理多播通信。

(3) ICMPv6 还增加了几个定义报文的功能及含义的其他协议

1) ND (Neighbor-Discovery)：邻站发现

2) MLD (Multicast Listener Delivery)：多播听众交付

-
- IP多播

1- IP multicast多播/组播的基本概念

1. IP多播：互联网上进行多播，靠路由器实现

(1) 能运行多播协议的路由器称为multicast router多播路由器
(2) 92年起，Multicast Backbone On the InterNEt多播主干网MBONE开始试验，现在已有相当大的规模了

2. 目的：更好的支持一对多通信（一个源点发到多个终点）
3. 多播IP地址：IP多播传送的分组使用的地址
   (1) 多播数据包的目的地址里写的是多播组的标识符
   (2) IPv4的每个D类地址对应一个多播组
   (3) 多播地址只能用于目的地址，不能是源地址
4. 多播数据报：首部协议字段值为2（IGMP）的数据报
   (1) 尽最大努力交付，不保证交给多播组所有成员
   (2) 不会产生ICMP差错报文，例：PING多播地址不会收到响应

2- 在局域网上硬件多播

1. IANA拥有的以太网地址块高24位为00-00-5E?
   (1) 规定IANA拥有的可用于以太网硬件地址的地址号只有后23位可变
   (2) 规定第8位为1时该地址为多播地址
   (3) 即实际以太网多播地址范围01-00-5E-00-00-00 ~ 01-00-5E-7F-FF-FF
2. d类IP地址前4位固定为1110，规定后28位中的后23位对应上一行的硬件地址
   (1) 因为d类IP地址后28位的前5位与硬件地址无关，因此在将多播IP地址与以太网硬件地址进行映射时可能需要IP层软件过滤

3- 网际组管理协议IGMP和多播组路由选择协议

1. IP多播两种协议
   (1) Internet Group Management Protocol网际组管理协议使路由器能知道多播组成员的信息
      1) 并不知道多播组的成员数，也不知道分布在哪些网络上，只需让多播路由器能知道其局域网上是否有主机加入或退出某多播组
   (2) 多播路由选择协议使多播路由器能互相协同工作、以最小代价传送多播数据包给组成员
      1) 需动态适应多播组成员的进出（不像ICMP只关注拓扑结构变化）
      2) 多播数据报可以由没加入多播组的主机发出，也可从非成员发出
      3) 转发时要考虑从哪来到哪去
2. 网际组管理协议IGMP
   (1) 和ICMP一样利用IP数据包传递报文，也向IP提供服务，一般视作网际协议IP的一个组成部分而不是一个单独的协议
   (2) 02年的rfc3376确立了IGMPv3为建议标准
   (3) 加入多播组：新入主机向该组多播地址发IGMP报文，多播路由器收到后，将新的组成员关系转发给互联网的其他多播路由器
   (4) 探询组成员变化：周期性（默认125秒）探询本地局域网的主机在最长响应时间N秒（默认为10）有没有响应，多次无响应后不将该组的成员关系转发给其他多播路由器
   (5) 主机和多播路由器间所有通信都使用IP多播；一个网络有多个多播路由器

时，只有其中一个会探询；只要有一个回答，其他的就可以不响应探询

3. 多播路由选择：找出以源主机为根的多播转发树
   (1) 洪泛与剪除法：适用于较小多播组，用洪泛广播转发多播数据报
      1) Reverse Path Broadcasting反向路径广播RPB：收到多播数据报时检查它是否是从源点沿最短（跳数）路径传来的，是的话才向其他地方转发，有多条最短路时选择IP地址最小的邻站
      2) 洪泛路径即为该源点的多播转发树
      3) 子结点方向无组成员时应剪除该结点及其子树；有新增组成员时再考虑接入到该多播转发树上
   (2) tunneling隧道技术：适用于地理位置上很分散的多播组
      1) 在进出不支持多播的网络时加上普通数据报的首部，封装成单播
      2) “出隧道”后再重新当作多播数据包，这种封装称为IP in IP
   (3) 基于核心的发现技术：适用于大范围的多播组
      1) 给多播组指定一个core核心路由器，给出其IP单播地址
      2) 发往该组的数据报都发给核心，再根据核心的转发树转发；若在发往核心路上恰经过目标路由器，则提前截获；有主机申请加入该组时，则用隧道技术向其转发各多播数据报的副本
   (4) 其他协议：Distance Vector Multicast Routing Protocol距离向量多播路由选择协议 DVMRP（RFC1075）、Core Based Tree基于核心的转发树 CBT（RFC2189，2201）、Multicast Extensions to OSPF开放最短通路优先的多播扩展 MOSPF（RFC1585）、Protocol Independent Multicast-Sparse Mode协议无关多播-稀疏方式 PIM-SM（RFC4601）、Protocol Independent Multicast-Dense Mode协议无关多播-密集方式 PIM-DM（RFC3973）

-
- 虚拟专用网 VPN和网络地址转换 NAT

1- Virtual Private Network虚拟专用网VPN
   (1) IP地址紧缺，一个机构实际申请到的IP地址数往往远小于机构内主机数
   (2) 互联网很不安全，机构内并不是所有主机都要接入到外部互联网
   (3) 仅在机构内使用的计算机可由使用TCP/IP的机构自行分配IP地址

1. 本地地址和全球地址
   (1) 本地地址：仅在机构内使用的IP地址，可由机构自行分配
   (2) 全球地址：全球唯一的，必须向互联网管理机构申请的IP地址
   (3) 为避免二义性，RFC1918指出了一些private address专用地址只用作本地地址，互联网中所有路由器不对这些目的地址的数据报进行转发
2. 三类本地专用IP地址/reusable address可重用地址
   (1) 10.0.0.0~10.255.255.255，即10.0.0.0/8，称为A类，24 位块
   (2) 172.16.0.0~172.31.255.255，即172.16.0.0/12，称为B类，20位块
   (3) 192.168.0.0~192.168.255.255，即192.168.0.0/16，称为C类，16位块
   (4) 专用网/专用互联网/本地互联网：采用专用IP地址的互联网络
3. 虚拟专用网VPN：利用公用互联网作为本机构各专用网间的通信载体的专用网
   (1) 虚拟：并没有使用通信专线
   (2) 专用：仅供本机构内的通信

(3) 因而可能需要解决加密问题和分析实际IP的问题

4. 隧道实现VPN：进出外部互联网时封装为普通数据报，路由器使用全球地址
5. intranet内联网：机构内部网络所构成的VPN
6. extranet外联网：机构内和外部机构共同建立的VPN
7. remote access VPN远程接入VPN：由VPN软件建立与公司内部主机间的VPN隧道

2- Network Address Translation网络地址转换NAT

1. 是94年申请新IP地址已基本不可能时提出的，让专用网用户连接互联网的方法
2. 装有NAT软件的路由器称为NAT路由器，它至少要一个全球地址
   (1) 使用本地地址的主机与互联网主机通信时，要让NAT路由器代为转换地址，（并计入地址转换表）再连接互联网
   (2) 离开专用网时替换源地址为全球地址
   (3) 进入专用网时替换目的地址为内部地址
   (4) NAT路由器有n个全球地址时，专用网内最多只有n台主机能同时接入互联网，否则需轮流使用NAT路由器
   (5) 专用网内部的主机只能发起向外的通信，自然不能充当服务器
3. Network Address ans Port Translation网络地址与端口号转换NAPT
   (1) 将运输层的端口号也利用上，使更多主机能同时使用NAT路由器
   (2) 为区分，将老的NAT称作traditional NAT

-
- 多协议标记交换MPLS

1. IETF于1997年成立了 MPLS 工作组，开发出一种新的协议——多协议标记交换 MPLS (MultiProtocol Label Switching)
   (1) “多协议”表示在 MPLS 的上层可以采用多种协议，例如：IP，IPX；可以使用多种数据链路层协议，例如：PPP，以太网，ATM 等
   (2) “标记”是指每个分组被打上一个标记，根据该标记对分组进行转发
2. 为了实现交换，可以利用面向连接的概念，使每个分组携带一个叫做标记 (label) 的小整数。当分组到达交换机（即标记交换路由器）时，交换机读取分组的标记，并用标记值来检索分组转发表。 这样就比查找路由表来转发分组要快得多
3. MPLS 并没有取代 IP，而是作为一种 IP 增强技术，被广泛地应用在互联网中。
4. MPLS 具有以下三个方面的特点：
   (1) 支持面向连接的服务质量；
   (2) 支持流量工程，平衡网络负载；
   (3) 有效地支持虚拟专用网 VPN。

1- MultiProtocol Label Switching工作原理

1. IP 分组的转发
   (1) 在传统的 IP 网络中，分组每到达一个路由器后，都必须提取出其目的地址，按目的地址查找路由表，并按照“最长前缀匹配”的原则找到下一跳的 IP 地址（请注意，前缀的长度是不确定的）。
   (2) 当网络很大时，查找含有大量项目的路由表要花费很多的时间。

(3) 在出现突发性的通信量时，往往还会使缓存溢出，这就会引起分组丢失、传输时延增大和服务质量下降。

2. MPLS协议下的转发
   (1) 在 MPLS 域的入口处，给每一个 IP 数据报打上固定长度“标记”，然后对打上标记的 IP 数据报用硬件进行转发。
   (2) 采用硬件技术对打上标记的 IP 数据报进行转发就称为标记交换。
   (3) “交换”也表示在转发时不再上升到第三层查找转发表，而是根据标记在第二层（链路层）用硬件进行转发。
3. MPLS 域 (MPLS domain) 是指该域中有许多彼此相邻的路由器，并且所有的路由器都是支持 MPLS 技术的标记交换路由器 LSR (Label Switching Router)
4. LSR 同时具有标记交换和路由选择这两种功能，标记交换功能是为了快速转发，但在这之前LSR 需要使用路由选择功能构造转发表。
5. 转发等价类 FEC (Forwarding Equivalence Class)：路由器按照同样方式对待的分组的集合（“按照同样方式对待”表示：从同样接口转发到同样的下一跳地址，并且具有同样服务类别和同样丢弃优先级等）
   (1) 划分 FEC 的方法不受什么限制，这都由网络管理员来控制，因此非常灵活。
   (2) 入口结点并不是给每一个分组指派一个不同的标记，而是将属于同样 FEC 的分组都指派同样的标记。
   (3) FEC 和标记是一一对应的关系。
   (4) 负载平衡：网络管理员采用自定义的 FEC 就可以更好地管理网络的资源，这种均衡网络负载的做法也称为流量工程 TE (Traffic Engineering) 或通信量工程。

2- MPLS工作过程

1. MPLS 域中的各 LSR 使用专门的标记分配协议 LDP 交换报文，并找出标记交换路径 LSP。各 LSR 根据这些路径构造出分组转发表。
2. 分组进入到 MPLS 域时， MPLS 入口结点把分组打上标记，并按照转发表将分组转发给下一个 LSR。给 IP 数据报打标记的过程叫做分类 (classification)。
3. 一个标记仅仅在两个标记交换路由器 LSR 之间才有意义。分组每经过一个 LSR，LSR 就要做两件事：一是转发，二是更换新的标记，即把入标记更换成为出标记。这就叫做标记对换 (label swapping)。
4. 当分组离开 MPLS 域时，MPLS 出口结点把分组的标记去除。再以后就按照一般分组的转发方法进行转发。
5. 上述的这种“由入口 LSR 确定进入 MPLS 域以后的转发路径”称为显式路由选择 (explicit routing)，它和互联网中通常使用的“每一个路由器逐跳进行路由选择”有着很大的区别。

3- MPLS首部的位置与格式

1. 位置
   (1) MPLS 并不要求下层的网络都使用面向连接的技术。
   (2) 下层的网络并不提供打标记的手段，而 IPv4 数据报首部也没有多余的位置存放 MPLS 标记。

(3) 这就需要使用一种封装技术：在把 IP 数据报封装成以太网帧之前，先要插入一个 MPLS 首部。

(4) 从层次的角度看，MPLS 首部就处在第二层和第三层之间。

2. 首部格式

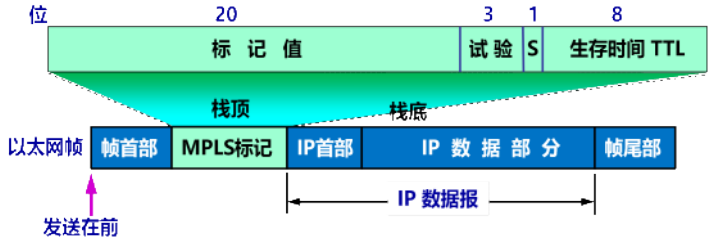
(1) 标记值（占 20 位）：可以同时容纳高达 220 个流（即 1048576 个流）。实际上几乎没有哪个 MPLS 实例会使用很大数目的流，因为通常需要管理员人工管理和设置每条交换路径。

(2) 试验（占 3 位）：目前保留用作试验。

(3) 栈S（占 1 位）：在有“标记栈”时使用。

(4) 生存时间TTL（占 8 位）：用来防止 MPLS 分组在 MPLS 域中兜圈子。

(5)



1)

2)

3)

4)

5)

6) ----------我是底线----------